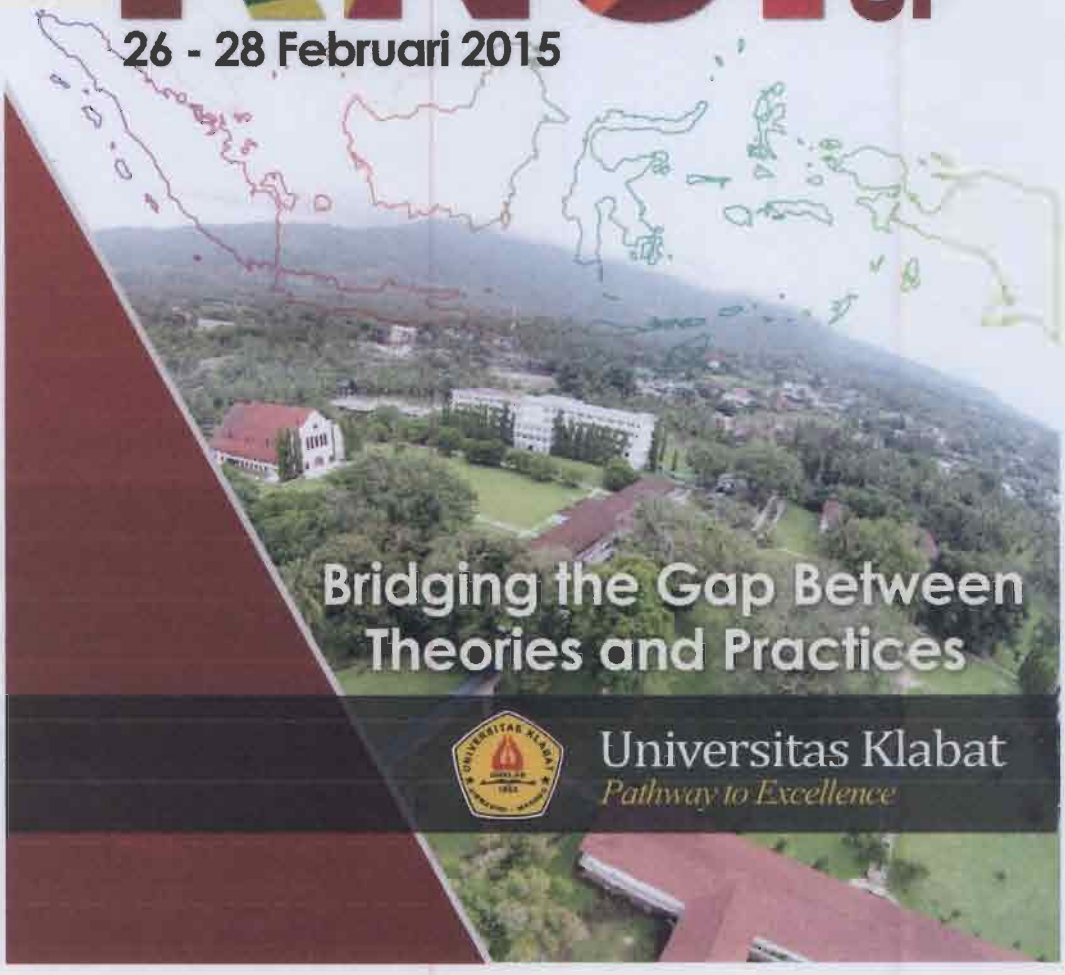
PROSIDING

Konferensi Nasional Sistem Informasi

KNSI 2015

26 - 28 Februari 2015



Bridging the Gap Between Theories and Practices

Universitas Klabat

Pathway to Excellence

Dipublikasikan Tahun 2015 Oleh:
Fakultas Ilmu Komputer – Universitas Klabat
Airmadidi, Minahasa Utara, Sulawesi Utara

ISSN : 1906-9613

Panitia Tidak Bertanggung Jawab Terhadap Isi Paper dari Peserta

PROSIDING
KONFERENSI NASIONAL SISTEM INFORMASI 2015

PERANCANGAN *BLUEPRINT* INFRASTRUKTUR SISTEM e-HEALTH DI RUMAH SAKIT UMUM DAERAH MAJALAYA

Doddy Ferdiansyah[1], Mokhamad Hendayun[2],Toto Suharto[3]

[1]Jurusan Magister Teknik Informatika, Fakultas Teknik, Universitas Langlangbuana
[2]Universitas Langlangbuana
[3]Universitas Langlangbuana
doddy2112@hotmail.com[1], hendayun@aol.de[2], tsuharto@gmail.com[3]

Abstrak

Sistem e-Health merupakan bagian dari kehidupan dari sistem perawatan *(Healthcare)* yang dibuat untuk membantu pasien untuk berinteraksi dengan dokter, administrasi, sampai dengan catatan medis pasien tersebut atau yang kita kenal dengan *Electronic Health Record* (EHR). EHR merupakan aset bagi sistem rumah sakit yang membangun sistem e-Health dan perlu mendapat pengamanan khusus karena mempunyai dampak yang sangat tinggi bagi rumah sakit itu sendiri maupun bagi pasien. Agar keamanan (*Confidentiality, Integrity, Availability*) dari EHR dapat ditingkatkan, maka dalam membangun infrastruktur sistem e-Health perlu menggunakan *blueprint* yang mengikuti standar sehingga dapat diakui secara internasional. Dalam perancangan *blueprint* infrastruktur sistem e-Health terdapat beberapa tahap yaitu melakukan identifikasi (aset, kerentanan, resiko dan dampak), membuat prioritas tingkat resiko, mencari control yang tepat terhadap resiko dengan tingkat yang sangat tinggi, dan memetakan kontrol tersebut terhadap sebuah kerangka *blueprint* infrastuktur. Hasil akhir dari penelitian ini merupakan sebuah rancangan *blueprint* infrastruktur sistem e-Health di Rumah Sakit Umum Daerah Majalaya dengan menggunakan standar-standar internasional yaitu ISO17799, ISO27799, ISO13335, dan NIST 800-30.

Kata Kunci : *blueprint, e-health, EHR, resiko*

1. Pendahuluan

1.1. Latar Belakang

Internet mempunyai peran yang sangat besar dalam kebutuhan manusia, terutama dalam bidang kesehatan. Saat ini, beberapa rumah sakit telah menggunakan sebuah sistem untuk melaksanakan beberapa kegiatannya seperti melakukan konsultasi jarak jauh, melihat catatan medis melalui web, dll. Electronic Health Record merupakan sebuah data/informasi yang sangat rahasia dan berharga yang tidal boleh diberikan kepada orang-orang yang tidak mempunyai hak terhadap EHR tersebut.

Sampai saat ini, sistem e-Health pada Rumah Sakit Umum Daerah (RSUD) Majalaya belum mempunyai blueprint keamanan, sehingga dalam penelitian ini penulis ingin mengangkat topik yang berhubungan dengan keamanan dari sistem e-Health tersebut.

1.2. Identifikasi Masalah

Berdasarkan uraian dari latar belakang, pada penelitian ini, terdapat masalah yang muncul yaitu pada sistem e-Health di Rumah Sakit Umum (RSUD) Majalaya belum mempunyai sebuah blueprint keamanan e-Health. Sehingga tanpa blueprint yang baik, sistem e-Health ini akan mendapat resiko yang sangat tinggi dari ancaman-ancaman yang dapat terjadi baik ancaman dari dalam maupun ancaman dari luar.

1.3. Tujuan

Dari masalah yang ada, maka tujuan dari penelitian ini adalah membuat sebuah blueprint keamanan sistem e-Health untuk Rumah Sakit Umum Daerah (RSUD) Majalaya. Akan tetapi dalam penulisan paper ini hanya menilai tingkat risiko yang perlu diterima untuk membuat blueprint keamanan sistem e-Health.

1.4. Metode Penelitian

Metode yang dilakukan dalam studi dan eksplorasi ini adalah sebagai berikut :

1. Studi Literatur

   Mencari dan mempelajari referensi mengenai :

   a. Konsep blueprint, penilaian resiko, pengendalian terhadap resiko, identifikasi aset, dampak, kerentanan.

b. Konsep keamanan informasi pada jaringan
c. Konsep sistem e-Health

2. Analisis
Melakukan penyelidikan atau pembelajaran lebih lanjut terhadap sistem e-health, aset apa saja yang harus dilindungi, kerentanan apa saja yang mungkin terjadi, dampak yang akan terjadi, resiko-resiko yang mungkin terjadi, kontrol-kontrol yang sesuai terhadap resiko tersebut.

2. Pemahaman Teori

2.1. Keamanan Jaringan

Menurut Simmonds, A; Sandilands, P; van Ekert, L keamanan jaringan terdiri dari ketentuan dan kebijakan yang diadopsi oleh seorang administrator jaringan untuk mencegah dan mengawasi akses yang tidak mempunyai ijin, penyalahgunaan, modifikasi, atau penyangkalan terhadap jaringan komputerdan sumber daya. Keamanan jaringan melibatkan otorisasi akses ke data dalam sebuah jaringan yang dikendalikan oleh administrator jaringan. User dapat memilih atau diberikan user ID dan password atau teknik otentikasi lainnya yang mengijinkan mereka untuk mengakses data/informasi dan program sesuai hak aksesnya. [SIM04]

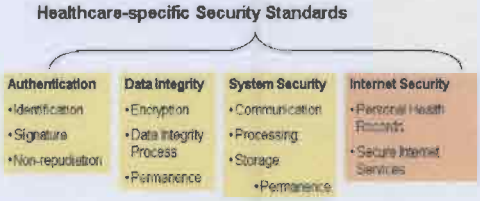
2.2. E-Health

Menurut World Health Organization (WHO) yang ditulis dalam websitenya (www.who.int , diakses 10 januari 2014), e-health adalah perpindahan dari sumber daya – sumber daya kesehatan dan perawatan kesehatan dengan menggunakan pendekatan elektronik. E-health tersebut mencakupi 3 area utama :

1. Menyampaikan informasi kesehatan, untuk health profesionals dah health consumers, melalui media jaringan public (internet) dan telekomunikasi.
2. Menggunakan kekuatan/kelebihan dari IT (information technology) dan e-commerce untuk meningkatkan layanan kesehatan public, contoh seperti melalui pendidikan dan pelatihan untuk health workers.
3. Penggunaan dari implementasi e-commerce dan e-business untuk dalam sistem pengolahan kesehatan (health system management).

e-health menawarkan sebuah teknologi baru dalam menggunakan sumber daya – sumber daya kesehatan seperti informasi, uang, dan obat-obatan, dan juga untuk meningkatkan efesiensi dalam menggunakan sumber daya tersebut. Internet juga menyediakan sebuah media baru sebagai penyebaran informasi., dan untuk berinteraksi dan berkolaborasi antara institusi, health profesionals, health providers dan masyarakat. [WHO14]

Sedangkan menurut C. Peter Waegemann, beberapa hal yang harus dilindungi menurut C. Peter Waegemann adalah keamanan terhadap kerahasiaan pasien, keamanan terhadap Electronic Health Record (EHR), dan keamanan terhadap sistem. Secara spesisfik, standar keamanan sebuah healthcare (e-health) dapat dilihat pada gambar 1. [PTW14]



Gambar 1. Standar keamanan sebuah *healthcare*

2.3. Electronic Health Record (EHR)

Menurut Laurinda B. Harman dan Kesa Bond dalam jurnal yang berjudul "Electronic Health Records : Privacy, Confidentiality, and Security" bahwa untuk memahami akan kompleksitas dari sistem electronic health records, akan sangat membantu untuk mengetahui sistem informasi kesehatan yang sudah, saat ini, harus menjadi apa. Catatan medis, baik kertas maupun elektronik, merupakan alat komunikasi yang mendukung pengambilan keputusan klinis, koordinasi pelayanan, evaluasi kualitas dan keberhasilan pelayanan, penelitian, perlindungan legal, pendidikan, dan proses akreditasi dan regulasi.

Kelemahan dari catatan medis yang berbasis kertas adalah kurangnya keamanan. Akses catatan medis dikendalikan dengan pintu, kunci, kartu identifikasi, dan prosedur sign-out yang membosankan bagi pengguna yang berwenang. Saat ini, tujuan utama dalam dokumentasi tetap sama, yaitu mendukung perawatan pasien. [LKB12]

2.4. Blueprint Arsitektur Keamanan

Menurut Gunnar Peterson dalam paper yang berjudul "Security Architecture Blueprint" menjelaskan bahwa tujuan dari tujuan utama dari blueprint arsitektur keamanan ini adalah untuk menfokuskan

terhadap daerah-daerah yang sangat penting dari sebuah organisasi, memperlihatkan keputusan dari kriteria dan konteks dalam setiap domain. Karena keamanan merupakan property dari sebuah sistem, maka akan sangat sulit bagi sebuah organisasi untuk memisahkan urusan yang berbeda pada lapisan sistem yang berbeda pula dan untuk memahami peran tersebut dalam sistem secara keseluruhan. [GUN06]

3. Lingkup Analisis

Rumah sakit umum daerah (RSUD) Majalaya adalah RSUD milik Pemda Kebupaten Bandung awalnya adalah Puskesmas yang dibangun pada tahun 1951 dan mulai dipergunakan tahun 1955, karena perkembangannya maka berkembang menjadi Rumah Sakit Tipe-D sejak tahun 1980, kemudian setelah memenuhi persyaratan sebagia Rumah Sakit dengan 4 Spesialisasi Dasar maka pada tahun 1988 Rumah Sakit ini mengalami transformasi menjadi Rumah Sakit Kelas-C yang ditetapkan oleh SK Menkes No.105/MENKES/SK/II/1988. RSUD Majalaya berlokasi di jalan cipaku No.87 kecamatan Paseh dengan menempati gedung dengan luas 7.069 m2 di atas lahan tanah seluas 27.890 m2. Salah satu fasilitas yang disediakan oleh RSUD Majalaya ini adalah sistem elektronik health (e-health) yang dibuat dengan aplikasi berbentuk web, seperti pada gambar 2.

Gambar 2. Tampilan aplikasi e-health RSUD Majalaya

Untuk mengakses sumber daya – sumber daya dari electronic health record (EHR), end user dapat menggunakan perangkat komunikasi apa saja (selama perangkat tersebut sesuai dengan spesifikasi sistem e-health) seperti laptop dan personal computer (PC), PDA / tablet, dan smartphone. Dengan perangkat-perangkat tersebut, user dapat masuk ke sistem e-health dengan melalui sebuah portal web (aplikasi) yang telah tersedia. Adapun beberapa layanan yang disediakan oleh sistem e-health adalah sebagai berikut :

1. Information & Public Services
2. E-clinical Services System
3. Teleconsultation
4. Decision Support System
5. Telemonitoring & Reporting
6. Teleeducation

Sebagai sumber daya yang terdapat pada electronik health record (EHR) terdapat beberapa jenis yang semuanya telah terintegrasi. Masing-masing sumber daya tersebut adalah sebagai berikut :

1. Sistem Administrasi Pasien
2. Sistem Perawatan Klinis
3. Sistem Laboratorium
4. Sistem Farmasi
5. Sistem DI/PACS
6. Sistem Telemonitoring
7. Sistem Lainnya

4. Menentukan Scope

Lingkup dari area keamanan dari sebuah organisasi perlu ditentukan untuk menentukan kebutuhan ISMS. Ada beberapa faktor yang utama untuk menentukan lingkup tersebut :

1. Area dari organisasi
2. Cakupan Lokasi
3. Aset, baik fisik atau lojik
4. Teknologi, termasuk hardware, jaringan, software, OS, dll

Berikut ini hasil dari penentuan lingkup dari sistem e-health pada rumah sakit umun daerah Majalaya dapat dilihat pada tabel 1.

Tabel 1. Lingkup dari sistem e-health

Area	Lokasi	Aset	Teknologi
Sistem E-Health	- Data center - Sistem IT dan jaringan pada rumah sakit, termasuk computer back-end yang terhubung pada sistem e-health	- Electronik Health Record (EHR) - Aplikasi / portal e-health - Server	- Server - Kamera / CCTV - Router dan Modem - Kabel jaringan, termasuk titik-titik pada computer back-end

5. Penilaian Resiko

Proses penilaian aset yang terdapat pada organisasi kesehatan merupakan langkah awal yang sangat penting dalam melakukan proses penilaian resiko. Hal ini juga dapat menghubungkan siapa yang bertanggungjawab terhadap aset-aset tersebut. Berikut hasil identifikasi aset pada sistem e-health RSUD Majalaya dapat dilihat pada tabel 2.

Tabel 2. Identifikasi aset

No	Aset	Jenis	Tanggungjawab
1	Electronic Health Record	Informasi	Dokter
2	Portal e-health	Aplikasi	Admin
3	Server	Fisik	Admin

Daftar ancaman-ancaman yang mungkin terjadi ini akan dapat digunakan pada proses penilaian ancaman. Ancaman dapat diakibatkan satu atau lebih kesengajaan (Deliberate), kebetulan (Accidental), atau lingkungan (Environmental). Daftar dibawah ini mengindikasikan setiap jenis ancaman dimana Deliberate (D), Accidental (A), dan Environment (E) saling relevan. D digunakan kepada semua tindakan yang disengaja yang mengarah pada aset IT, A digunakan kepada semua tindakan manusia yang secara kebetulan dapat merusak aset IT, dan E digunakan kepada semua insiden yang tidak berhubungan dengan tindakan dari manusia. Daftar ancaman dapat dilihat pada tabel 3.

Tabel 3. Daftar ancaman

No	Ancaman	Penyebab
1	Penyamaran (insider, ISP, Outsider)	D
2	Penggunaan yang tidak sah terhadap aplikasi informasi kesehatan	D, A
3	Perangkat lunak yang merusak	D, A
4	Penyusupan pada saluran komunikasi	D
5	Intersepsi pada saluran komunikasi	D
6	Kegagalan koneksi	D, A, E
7	Kesalahan routing	A
8	Kegagalan dari host, tempat penyimpanan, dan infrastruktur	D, A
9	Kesalahan operator	D, A
10	Kesalahan pemeliharaan (maintenance)	D, A
11	Kesalahan pengguna	D, A
12	Pencurian (insider, outsider)	D
13	Kerusakan (insider, outsider)	D, A

Beberapa ancaman yang sudah diidentifikasi akan memunculkan kerentanan-kerentanan (vulnerabilities) terhadap aset atau sistem informasi kesehatan. Daftar dibawah ini menunjukan beberapa kerentanan yang terdapat dalam area-area keamanan, termasuk ancaman mana yang akan dieksploitasi oleh kerentanan tersebut. Daftar kerentanan dapat dilihat pada tabel 4.

Tabel 4. Daftar kerentanan

No	Vulnerabilites	Ancaman
1	Antarmuka pada aplikasi yang sangat kompleks	Kesalahan Pengguna
2	Kurang efisien pengendalian pada perubahan konfigurasi	Kesalahan Operator
3	Kurangnya pemeliharaan atau kesalahan instalasi pada media penyimpanan	Kesalahan Pemeliharaan
4	Tidak ada atau kurangnya testing terhadap aplikasi	Penggunaan yang tidak sah terhadap aplikasi informasi kesehatan
5	Tidak adanya pengendalian pada download dan penginstalan program/aplikasi	Perangkat lunak yang merusak
6	Kurangnya mekanisme identifikasi dan autentikasi pada pengguna	Penyamaran
7	List pada tabel password yang tidak dilindungi	Penyamaran
8	Manajemen password yang jelek	Penyamaran
9	Kurangnya dokumentasi	Kesalahan Operator
10	Jalur komunikasi yang tidak dilindungi	Intersepsi pada saluran komunikasi, Penyusupan pada saluran komunikasi
11	Tempat penyimpanan yang tidak dilindungi	Pencurian
12	Kurangnya pelatihan terhadap penggunaan aplikasi	Kerusakan
13	Respon pada pelayanan pemeliharaan yang tidak memadai	Kegagalan dari host, tempat penyimpanan, dan infrastruktur
14	Tidak mengikuti prosedur pada instalasi atau konfigurasi perangkat	Kesalahan routing
15	Tidak ada anti virus pada perangkat	Perangkat lunak yang merusak
16	Tidak ada jalur back up jika terjadi koneksi terputus	Kegagalan koneksi

Pada pengidentifikasian dari poin-poin sebelumnya, aset-aset yang mempunyai nilai dan mempunyai beberapa tingkat dari kerentanan sangat beresiko apabila ancaman terhadap aset-aset tersebut ada. Penilaian pada resiko merupakan sebuah kombinasi dari potensi dampak bisnis yang merugikan dari insiden yang tidak diinginkan, dan tingkat ancaman dan kerentanan yang dinilai. Penilaian resiko dapat dilihat pada lampiran nomor 1.

Pada kriteria penilaian matriks diatas, nilai dari resiko dibagi menjadi tiga tingkatan, yaitu Low, Medium, High dengan kriteria penilaian sebagai berikut :

- Nilai 1 – 3 : Low
- Nilai 4 – 5 : Medium
- Nilai 6 – 7 : High

Pengendalian resiko dapat dilihat pada lampiran nomor 2.

6. Blueprint Infrastruktur Sistem e-Health RSUD Majalaya

Sebuah blueprint atau biasa disebut dengan referensi arsitektur menyediakan lingkup dengan tingkat yang tinggi dan definisi kebutuhan e-health dari pandangan secara arsitektural. Arsitektur ini dimaksudkan untuk :

- Menyediakan sebuah framework untuk mengimplementasikan strategi e-health RSUD Majalaya dan road map bagi para investor, pembangun dan manejer untuk rencana 10 tahun kedepan
- Menyediakan klasifikasi yang lengkap terhadap informasi, komponen teknologi dan layanan-layanan yang akan membutuhkan kesadaran tentang visi dari sistem e-health RSUD Majalaya
- Menyediakan struktur yang umun (taxonomy) dan bahasa (semantics) untuk sistem e-health di RSUD Majalaya

Beberapa model konsep pada penelitian ini mengacu kepada standar model Ontario's e-health. Model konsep yang digunakan pada Ontario seperti gambar 3 : [ONT14]

Gambar 3. Model Konsep e-Health Ontario

7. Kesimpulan

Kesimpulan dari hasil penelitian ini adalah dari hasil penilaian resiko, EHR mendapatkan prioritas utama dalam pengendalian terhadap resiko itu sendiri. Terdapat 5 resiko dengan tingkat sedang, dan 3 resiko dengan tingkat tinggi. Yang paling berbahaya adalah pada bagian koneksi (media transmisi) dan identifikasi otentikasi terhadap pengguna yang mengakses EHR. Sehingga didalam sistem e-health perlu adanya sebuah mekanisme untuk melakukan otentikasi dan akses control.

Daftar Pustaka:

[GUN06] Peterson, Gunnar. (2006) "Security Architecture Blueprint". Arctec Group. [Online]. Tersedia : http://www.arctecgroup.net/pdf/ArctecSecurityArchitectureBlueprint.pdf

[LKB12] Harman, Laurinda B., Bond, Kesa. (2012) "Electronic Health Records : Privacy, Confidentiality, and Security". [Online]. Tersedia : http://virtualmentor.ama-assn.org/2012/09/stas1-1209.html

[ONT14] Ontario, ehealth. (2014) "Ontario's eHealth Blueprint". [Online]. Tersedia : http://www.ehealthontario.on.ca/architecture/education/courses/educationdownloads/Blueprint-Narration.pdf

[PTW14] Waegemann, C. Peter. (2014) "Confidentiality and Security for e-Health". [Online]. Tersedia : www.itu.int/itudoc/itu-t/workshop/e-health/s5-05_pp7.ppt

[SIM04] Simmonds, A; Sandilands. P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science.

[WHO14] WHO, World Health Organization. (2014) "E-Health". [Online]. Tersedia : http://www.who.int/trade/glossary/story021/en/